UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/771,840	02/04/2004	Art Shelest	MSFT121932	9753

26389 7590 04/17/2008
CHRISTENSEN, O'CONNOR, JOHNSON, KINDNESS, PLLC
1420 FIFTH AVENUE
SUITE 2800
SEATTLE, WA 98101-2347

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
04/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/771,840	SHELEST ET AL.	
	Examiner	Art Unit	
	JUNG KIM	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 December 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51,53,56 and 60-63* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-51, 53, 56 and 60-63* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the amendment filed on 12/26/07.

2. Claims 1-51, 53, 56 and 60-63 are pending.

3. Claims 60-63 are new.

Response to Arguments

4. Applicant's arguments have been fully considered but they are not persuasive. With respect to claim 1, applicant argues that Sobel merely discloses a locally installed compliance verification and does not disclose a clean group server. (Remarks, pg. 12) As outlined below in the rejections, Sobel discloses a Compliance Registration Manager and DHCP Proxy which are functionally equivalent to the limitation "clean group server" and which perform the method steps as listed in the claim and the respective dependent claims.

5. With respect applicant's arguments that Sobel's disclosure of a DHCP server does not anticipate a domain controller, (pg. 13, 2nd paragraph) this argument is not persuasive because the DHCP server of Sobel effectively segregates a client to one of two domains: a protected network or a restricted network depending on the results of a compliance check on the client. Furthermore, applicant's specification merely identifies a domain controller as being a "part of the infrastructure that participates in the clean group maintenance." (pg. 10, lines 10-12) Hence, under the broadest reasonable interpretation of the claim, Sobel suggests a domain controller. MPEP 2111.

6. Applicant further argues that Sobel does not disclose disabling or enabling the computer domain account, placing the computer's domain account in a disabled state until the computer is proved to be in compliance, or requiring the clean group server to participate in the domain join operation. (pg. 15) However, as outlined below, Sobel suggest the aforementioned limitations. In particular, Sobel discloses providing network access to a client to a protected VLAN when the client is found to be compliant; if the client is not found to be compliant, access to the protected VLAN is prohibited until it is determined that the client is compliant. Paragraphs 24-26.

7. With respect to applicant's arguments that neither Sobel nor Herrmann discloses the new limitations of amended claim 39, these arguments do not consider Sobel and Herrmann in view of Lineman, which is the basis for the 103 rejection.

8. Finally, with respect to applicant's argument that the prior art does not disclose providing access to IPsec settings by binding active directory group policy to the clean group membership such that only members of the clean group can read the policy, this argument is not persuasive for the following reasons: as outlined below, Lineman suggests providing limited access to published security policies by preparing security policy documents and publishing these documents, wherein only specified users with defined roles have access to a particular published document. This feature effectively prevents users who do not have the proper access privileges to read the security policies and thereby prevent unauthorized users from attaining the privileges reserved for specific roles. Paragraph 70. Furthermore, it is notoriously well known in the art to establish IPsec configuration information in shared security policies. For example,

Microsoft's Active Directory enables centralized IPsec configuration. A client, who does not have privileged access to a policy document having IPsec configuration information, will not have access to the IPsec configuration information. Hence, the prior art suggest the limitation of providing access to IPsec settings by binding active directory group policy to the clean group membership such that only members of the clean group can read the policy.

9. Applicant's remaining arguments are cumulative to those discussed above. Hence, for these reasons, claims 1-51, 53, 56 and 60-63 remain rejected.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. Claims 1-9, 11-38 and 60-63 are rejected under 35 USC 102(e) as being anticipated by Sobel et al. US Patent Application Publication No. 20040103310 (hereinafter Sobel).

12. As per claims 1-9 and 11-14, 60, 62 and 63, Sobel discloses a method for providing security in a computer system, comprising:

a. selecting a set of properties for use in determining if an item is clean (paragraph 20);

b. evaluating an item to determine if it has the specified set of properties

c. sending an add request to a clean group server (paragraph 24 and 25; "if 325 the requesting client 105 is compliant with the security policies, the DHCP proxy 110 requests 330 an IP address from the DHCP server 150 on the protected network 140"; Compliance Registration Manager and DHCP Proxy are functionally equivalent to the limitation "clean group server");

d. if the clean group server determines that the item has the specified set of properties, the clean group server designating the item as a member of a clean group (paragraph 25);

e. wherein the items are computers (paragraph 13);

f. wherein when a computer is to be evaluated, a clean component is installed on the computer to perform compliance checks (paragraph 19);

g. wherein a compliance check is performed at a selected time for an item to determine if the item has the specified set of properties (paragraph 20 and 24);

h. wherein one of the specified set of properties is whether all of the available updates have been installed (paragraph 17);

i. wherein the updates comprise at least one of security updates or service packs (paragraph 17);

j. wherein if the compliance check fails, a message is sent to indicate that the object should not be in the clean group; (paragraphs 21 and 24)

k. wherein if the compliance check fails, the clean group membership of the item is invalidated (paragraphs 21 and 24-27);

l. wherein the invalidation of the clean group membership comprises local actions including at least hiding the domain credentials of the item. (paragraph 25; item is segregated into a restricted network)

m. wherein if a compliance check passes, a message is sent to provide information that will be evaluated to determine if the item should be in the clean group (paragraphs 25 and 26);

n. wherein after a message is received and a determination is made that the item should be in the clean group, a countdown is started and if another message is not received by the end of the countdown, the item is removed from the clean group (paragraph 25; a timeout feature is inherent in connection oriented communications);

o. wherein an item in the clean group performs a self check to determine if it still has the specified set of properties, and if it does not, takes action to have itself removed from the clean group; (paragraph 24);

p. wherein the clean group server initiates a status check to determine if the members in the clean group still have the specified properties (paragraph 20);

q. wherein if the clean group server determines that the item does not have the specified set of properties, the clean group server designates the item as a member of a dirty group (paragraph 26);

r. wherein the invalidation of the clean group membership comprises local actions including at least erasing the domain credentials of the item; (paragraphs 20, 27, 33)

s. wherein if the compliance check fails, additional steps are taken including at least logging out a privileged user. (paragraphs 20, 27, 33)

13. As per claims 15-25 and 61, Sobel discloses a system for managing security, comprising:

t. A clean group server; (Compliance Registration Manager and DHCP Proxy are functionally equivalent to the limitation "clean group server)

u. an update component which includes updates for items; (paragraph 14)

v. a clean runtime component, the clean runtime component being installed on an item and being able to communicate with the update component and the clean group server; and if the clean group server determines that the item has a specified set of properties, the clean group server designates the item as a member of a clean group; (paragraph 19)

w. further comprising a domain controller with which the clean group server communicates to designate the item as a member of the clean group; (fig. 1, reference nos. 110, 115, 120, 125, 130, 135)

x. wherein the items comprise computers (paragraph 13);

y. wherein compliance checks are performed for the items to determine if the items meet the selected criteria; (paragraph 20)

z. wherein one of the criteria is whether selected available updates have been installed; (paragraph 17)

aa. wherein the updates comprise at least one of security updates or service packs; (paragraph 17)

bb. wherein if a compliance check fails, a message is sent from the clean runtime component to the clean group server to indicate that the item should not be in the clean group; (paragraphs 21 and 24)

cc. wherein if the compliance check passes, a message is sent from the clean runtime component to the clean group server to provide information that will be used to evaluate whether the item should be in the clean group; (paragraphs 25 and 26)

dd. wherein after a message is received to indicate that the item should be placed in the clean group, a countdown is started and if another message is not received by the end of the countdown, the item is removed from the clean group; (paragraph 25; a timeout feature is inherent in connection oriented communications)

ee. wherein the clean runtime component performs a self-check of the item to determine if it meets the selected criteria for remaining in the clean group; (paragraph 24)

ff. wherein the clean group server initiates a compliance check for items to determine if they should remain in the clean group; (paragraph 20)

gg. wherein if the clean group server determines that the item does not have the specified set of properties, the clean group server designating the item as a member of a dirty group. (paragraph 26)

14. As per claims 26-32, Sobel discloses one or more computer-readable media having computer-executable components for providing security in a computer system, the computer-executable components (paragraph 5) comprising:

hh. a runtime object for installation on a computer, wherein the runtime object, when executed, determines if the computer has a specified set of properties, and sends an add request to a clean group server; (paragraphs 19-21)

ii. instructions for installation on a clean group server for processing the add request, wherein the instructions, when executed, cause the clean group server to designate the computer as a member of a clean group, if the clean group server determines that the add request is valid; (paragraphs 24-26)

jj. wherein the compliance check is performed initially upon installation of the runtime object; (paragraph 19)

kk. wherein the compliance check comprises a determination of whether selected available updates have been installed on the computer; (paragraph 17)

ll. wherein the selected available updates comprise at least one of security updates or service packs; (paragraph 17)

mm. wherein after the add request is received by the clean group server, a countdown is started and if another message is not received by the end of the

countdown, the computer is removed as a member of the group; (paragraph 25; a timeout feature is inherent in connection oriented communications)

nn. wherein the clean runtime object initiates a compliance check on the computer (paragraph 20);

oo. wherein the clean group server communicates with the runtime object to initiate a compliance check (paragraphs 19 and 20).

15. As per claims 33-38, Sobel discloses a method for providing security in a computer system, comprising:

pp. Selecting a set of properties for use in determining if a computer is clean (paragraph 12);

qq. Evaluating a computer to determine if it has the specified set of properties;

rr. Sending an add request to a clean group server (paragraphs 22-24); and

ss. based on whether or not the clean group server determines that the computer is in compliance, the clean group server disabling or enabling the computer domain account; (paragraph 24-26)

tt. wherein when a new computer is to be added to the domain account, the new computer's account is placed in a disabled state until the computer is proved to be in compliance; (paragraphs 20, 21, 24 and 25)

uu. wherein when a new computer is to be added to the domain account, the domain join operation is predicated on proving that the computer is in compliance

by requiring the clean group server to participate in the domain join operations; (paragraph 21)

vv. wherein evaluating a computer comprises determining whether available updates have been installed on the computer (paragraph 14);

ww. wherein the computer periodically performs compliance checks; (paragraphs 20 and 24)

xx. wherein the clean group server periodically initiates a compliance check on the computer (paragraphs 20 and 24).

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. Claim 10 is rejected under 35 USC 103(a) as being unpatentable over Sobel.

18. As per claim 10, the rejection of claim 7 under 35 USC 102(e) as being anticipated by Sobel is incorporated herein. Sobel further discloses that if the compliance check fails, the client is not given access to the protected network. (paragraph 26) The inability to access resources on the protected network disables the client from connecting with these resources via any secure connections using standard techniques such as SSL or VPN. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to hide cryptographic keys if the

compliance check fails because the client is denied access to these resources. The aforementioned cover the limitations of claim 10.

19. Claims 39-47, 51, 53 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sobel in view of Lineman et al. US Patent Application Publication No. 20030065942 (hereinafter Lineman).

20. As per claims 39-47, 51 and 53, the rejection of claim 52 under 35 USC 102(e) as being anticipated by Sobel is incorporated herein.

yy. performing compliance checks for items; placing items which pass the compliance check into a clean group; and removing items from the clean group which fail the compliance check; (Abstract; paragraph 12)

zz. wherein after an item passes a compliance check and is placed in the clean group, a countdown is started and if another compliance check is not passed by the end of the countdown, the item is removed from the clean group; (paragraph 25; a timeout feature is inherent in connection oriented communications)

aaa. wherein the item is a computer; (paragraph 13)

bbb. wherein the item performs a compliance check; (paragraphs 20 and 24)

ccc. wherein a clean group server initiates a compliance check on the item; (paragraphs 20 and 24)

ddd. wherein the compliance check is performed by the item communicating with an update Web site to determine if updates are available for the item; (paragraphs 14 and 17)

eee. wherein the item communicates with a clean group server to establish its membership in the clean group; wherein the clean group server communicates with a domain controller; (fig. 1, reference nos. 110, 115, 120, 125, 130, 135)

fff. wherein a compliance check is initiated by one or more of a client coming online, changes in client status/configuration, changes in network status/configuration, or changes to a compliance policy; (fig. 3)

ggg. wherein an item is a user, and a user's clean group membership is evaluated on the basis of whether the user's computer is in compliance. (paragraph 12)

21. Sobel does not disclose wherein the clean group is utilized to provide enforcement of the computer security policy by binding active directory group policy to the group membership such that only members of the group can read the policy; wherein items within the clean group can access a collection of IPSec communication requirements and parameters that allow them to communicate with other items within the clean group; and items not within the clean group cannot access the collection of IPSec communication requirements and parameters, and are thereby quarantined from receiving information from or sending information to items within the clean group. Lineman discloses a method and apparatus for managing security policies, including a common feature to provide limited access to published security policies that include the

following steps: preparing security policy documents and publishing these documents, wherein only specified users with defined roles have access to a particular published document. This feature effectively prevents users who do not have the proper access privileges to read the security policies and thereby prevent unauthorized users from attaining the privileges reserved for specific roles. Paragraph 70. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Sobel to enforce the computer security policy by binding active directory group policy to the group membership such that only members of the group can read the policy; wherein only computers which comply with the policy and are thus members of the clean group can read the policy parameters and thus communicate with one another, while computers which are not members of the clean group are effectively prevented from communicating with computers in the clean group, thus in effect providing a quarantine mechanism. One would be motivated to do so to significantly enhance the communication of these security policies to the users. Lineman, ibid.

22. Finally, Sobel does not disclose the security policy provides IPSec communication requirements and parameters. However, it is notoriously well known in the art that IPSec communications provides secure communications between a sender and a receiver to ensure that communications are not monitored by an unscrupulous 3rd party. In addition, IPSec protocols operate in the network layer to provider greater flexibility over other secure protocols such as SSL. For example, Microsoft's Active Directory, which provides centralized management and configuration of computers, enables centralized IPsec configuration for secure communications between computers

configured via the Active Directory. Examiner takes Official notice of this teaching. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the security policy to provide IPSec communication requirements and parameters. One would be motivated to do so to provide flexible and secure communication between a sender and a receiver. The aforementioned cover the limitations of claims 39-47, 51 and 53.

23. As per claim 56, the rejection of claim 39 under 35 USC 103(a) as being unpatentable over Sobel in view of Lineman is incorporated herein. Sobel does not expressly disclose wherein a client that changes state from membership in the clean group to non-membership is required to clear all policy settings distributed via the clean group. However, it is notoriously well known in the art at the time of invention to invalidate policy settings when a client is no longer part of a group. For example, users access means, such as passwords and usernames are conventionally deactivated or deleted by an administrator when a user is removed as a client. Examiner takes Official notice of this teaching. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Sobel to include the step of wherein a client that changes state from membership in the clean group to non-membership is required to clear all policy settings distributed via the clean group. One would be motivated to do so to prevent access by a user whose privileges have been revoked as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 56.

24. Claims 39, 41-53 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herrmann et al. US Patent Application 20040107360 (hereinafter Herrmann) in view of Lineman.

25. As per claims 39, 41-49, 51 and 53 Herrmann discloses a method for providing security in a computer system, comprising:

hhh. performing compliance checks for items; placing items which pass the compliance check into a clean group; and removing items from the clean group which fail the compliance check; (paragraph 96)

iii. wherein the item is a computer; (fig. 4, reference no. 310)

jjj. wherein the item performs a compliance check; (paragraph 94)

kkk. wherein a clean group server initiates a compliance check on the item; (paragraphs 93-95)

lll. wherein the compliance check is performed by the item communicating with an update Web site to determine if updates are available for the item; (paragraphs 79 and 97)

mmm. wherein the item communicates with a clean group server to establish its membership in the clean group; (paragraph 76-79 and 93-95)

nnn. wherein the clean group server communicates with a domain controller; (fig. 4, reference nos. 320, 330, 440, 450 and 460);

ooo. wherein a compliance check is initiated by one or more of a client coming online, changes in client status/configuration, changes in network status/configuration, or changes to a compliance policy; (fig. 7A, reference no. 701)

ppp. wherein a clean group server communicates to non-compliant items how to get back into compliance; (paragraph 79 and 97)

qqq. wherein the non-compliant items are directed to a Web site with online instructions to the user, and once the instructions are followed, another server-assisted compliance check is initiated; (paragraph 79 and 97)

rrr. wherein an item is a user, and a user's clean group membership is evaluated on the basis of whether the user's computer is in compliance. (fig. 4, reference no. 310 and related text)

26. Herrmann does not disclose wherein the clean group is utilized to provide enforcement of the computer security policy by binding active directory group policy to the group membership such that only members of the group can read the policy; wherein items within the clean group can access a collection of IPSec communication requirements and parameters that allow them to communicate with other items within the clean group; and items not within the clean group cannot access the collection of IPSec communication requirements and parameters, and are thereby quarantined from receiving information from or sending information to items within the clean group. Lineman discloses a method and apparatus for managing security policies, including a common feature to provide limited access to published security policies that include the

following steps: preparing security policy documents and publishing these documents, wherein only specified users with defined roles have access to a particular published document. This feature effectively prevents users who do not have the proper access privileges to read the security policies and thereby prevent unauthorized users from attaining the privileges reserved for specific roles. Paragraph 70. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Herrmann to enforce the computer security policy by binding active directory group policy to the group membership such that only members of the group can read the policy; wherein only computers which comply with the policy and are thus members of the clean group can read the policy parameters and thus communicate with one another, while computers which are not members of the clean group are effectively prevented from communicating with computers in the clean group, thus in effect providing a quarantine mechanism. One would be motivated to do so to significantly enhance the communication of these security policies to the users. Lineman, ibid.

27. Finally, Herrmann does not disclose the security policy provides IPSec communication requirements and parameters. However, it is notoriously well known in the art that IPSec communications provides secure communications between a sender and a receiver to ensure that communications are not monitored by an unscrupulous 3rd party. In addition, IPSec protocols operate in the network layer to provider greater flexibility over other secure protocols such as SSL. For example, Microsoft's Active Directory, which provides centralized management and configuration of computers, enables centralized IPsec configuration for secure communications between computers

configured via the Active Directory. Examiner takes Official notice of this teaching. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the security policy to provide IPSec communication requirements and parameters. One would be motivated to do so to provide flexible and secure communication between a sender and a receiver. The aforementioned cover the limitations of claims 39, 41-49, 51 and 53.

28. As per claim 50, the rejection of claim 48 under 35 USC 102(e) as being anticipated by Herrmann is incorporated herein. Herrmann does not disclose wherein the non-compliant items are instructed how to get into the compliant state automatically without requiring a user's involvement. However, automation of a step is deemed to be an obvious enhancement. In re Venner, 262 F.2d 91, 95, 120 USPQ 193, 194 (CCPA 1958). It would be obvious to one of ordinary skill in the art at the time of invention to modify the invention of Herrmann to include the feature wherein the non-compliant items are instructed how to get into the compliant state automatically without requiring a user's involvement. One would be motivated to do so to replace the manual activity with an automatic means of making the non-compliant item to be compliant as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 50.

29. As per claim 56, the rejection of claim 39 under 35 USC 103(a) as being unpatentable over Herrmann in view of Lineman is incorporated herein. Herrmann does not expressly disclose wherein a client that changes state from membership in the clean

group to non-membership is required to clear all policy settings distributed via the clean group. However, it is notoriously well known in the art at the time the invention was made to invalidate policy settings when a client is no longer part of a group. For example, users access means, such as passwords and usernames are conventionally deactivated or deleted by an administrator when a user is removed as a client. Examiner takes Official notice of this teaching. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Herrmann to include the step of wherein a client that changes state from membership in the clean group to non-membership is required to clear all policy settings distributed via the clean group. One would be motivated to do so to prevent access by a user whose privileges have been revoked. The aforementioned cover the limitations of claim 56.

Conclusion

30. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JUNG KIM whose telephone number is (571)272-3804. The examiner can normally be reached on FLEX.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Primary Examiner AU 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132